DFL-210/800/1600/2500 Firmware Release Note

Firmware: 2.11.02
Date: November 1, 2006

Changes from DFL-210/800/1600/2500 v2.05.00 to v2.11.02

Important note

Firmware 2.11.02 uses a new configuration format. The new format is not compatible with the format used in 2.05 and earlier. These configuration files will be automatically converted to the new format during the first start-up. Older firmware (2.00 - 2.05) can not understand the new format.

Customers that had firmware 2.00 - 2.05 factory installed can use reset-to-factory to restore their firmware from 2.11 to 2.0x.

Customers with firmware 2.11 and later factory installed can not downgrade to 2.00 - 2.05.

All users are encouraged to make a backup of the configuration before upgrading to firmware 2.11.02.

Bug fixes

#2873 The L2TP server could not handle incoming L2TP client requests sent over IPsec if the clients were located behind the same NAT gateway.

#4010 L2TP implementation incompatible with some other L2TP implementations. For one, the L2TP server failed to establish a tunnel with the L2TP client in D-Link DI-604.

Affects DFL-210 and DFL-800.

#3322 PPTP server sometimes failed to send any traffic at all through a newly connected tunnel. Packets could only be sent from the client to the server, not from the server to the client. The PPTP client had to be reconnected one

or more times before traffic could be sent in both directions through the tunnel.

Affects dfl 2.00.00 and up

#3783 During high load using SLB and Stickiness the firewall may have malfunctioned.

Affects dfl 2.00.00 and up

Changes

The IPsec engine has been upgraded.

#3483 The CLI has been upgraded and do now have configuration possibilites.

The configuration format and engine has changed. The new format is not compatible with the old one. Configuration files from 2.05 and earlier will be automatically converted to the new format during first start-up.

#3387 SSH server has been added. Remote management is now possible via SSH and the CLI.

A SSH keygenerator has been added. Can be found under Tools->SSH-Keygen

#3399 IDS (Intrusion Detection System) has been renamed to IDP (Intrusion Detection and Prevention).

The IDP engine has been upgraded and enhanced.

An advanced IDP service is available from D-Link. The new service has fast and frequent updates (up to several updates per day). More information can be found on D-Links security portal (http://security.dlink.com.tw).

TCP pseudo reassembly has been added. IDP scanning is now stream based instead of packet based.

#3107 The log system has been enhanced. All log messages have been assigned unique IDs. The ID number can be used to find more information about the log message from the Log Reference Guide (available for download from D-Link).

A new folder has been added under Objects, called "Authentication Objects". Pre-shared keys (previously found under "Objects->VPN Objects->Pre-Shared Keys"), Certificates (previously found under "Objects->X.509 Certificates") and SSH Client keys (new) can be configured here.

The "Traffic Shaping" folder has been moved to a new folder called "Traffic Management".

"Threshold rules" has been moved to the new "Traffic Management" folder.

A new drop down menu, called "Maintenance", has been added in the toolbar. Backup, reset and upgrade have been moved to this menu. New items are "Update Center", "License" and "Tech support". The last one can be used in contact with D-Link support to provide information about the firewall while troubleshooting.

#2925 Blacklisting has been added.

#1054 Ethernet interfaces are not reset during activation of new configuration settings.

#3097 DHCP packets (UDP port 67/68) sent through the firewall will be dropped if there is no DHCP relayer configured. DHCP packets can not be forwarded using the IP ruleset.

#3989 DES-3626 (R4.01-B19 or later) and DES-3550 (R4.01-B19 or later) are now also supported by ZoneDefense. 4.xx firmware is recommended for these two switches, since firewall-switch communication is faster than with 3.xx switch firmware.

IDP log messages in Mem-Log and SMTP-Log now include a link to the

advisory information on D-Link's security portal.

For more details of new features download the new user manual, CLI reference guide and log reference guide from D-Link's website.

Firmware: 2.05.00
Hardware: A1
Date: May 18, 2006

Changes from DFL-210/800/1600/2500 v2.04.00 to v2.05.00

Bug fixes

#2816 When the first IPsec tunnel was configured and saved, no traffic could be sent though the tunnel until the firewall was restarted. When the firewall stated up without any configured tunnels, the crypto accelerator was not initialized correctly.

Affects DFL-1600/2500.

#2922 The firewall was not rebooted (restarted from power on state) after a firmware upgrade. If the upgrade package included a new loader the new version was not used until next reboot.

Affects dfl-2.00 and up.

#3091 IPsec keepalive did not work. The IPsec tunnel would be taken down as no response is received on the keepalive packets.

Affects dfl-2.03 and up.

#3186 Promiscuous mode was enabled by default on all interfaces. The firewall would pick up packets that do not have the DFL as destination, leaving the DFL to process packets that will be dropped anyway.

Affects dfl-2.00 and up.

#3208 TCP connections to the DFL itself (webUI, ALGs, PPTP) did not obey received TCP MSS.

Affects dfl-2.00 and up.

#3350 Appliances that was rebooted due to software issued reboot or a core crash

may have failed to reboot correctly, leaving the unit unreachable. The only way to reboot it correctly from this unreachable state is to do a hard reboot by cutting the power and then put the power back on.

Affects DFL-800, dfl-2.00 and up.

#3353 It was not possible to change date or time if the new month was December.

Affects dfl-2.00 and up.

#3360 The firewall could crash if an IP address was used as ID in an ID-list.

Affects dfl-2.00 and up.

#3376 Blacklist items on position x and later did not get blocked. The number of working blacklist items depended on the URLs configured, but usually somewhere between 25 and 30.

Affects dfl-2.00 and up.

#3385 The firewall could crash if IDS rules were deleted and the configuration was saved and activated.

Affects dfl-2.00 and up.

#3392 The IDS engine could hang the firewall, given an improper signature database.

Affects dfl-2.00 and up.

#3399 After a reset-to-factory from the webUI, the browser in some cases tried to reconnect to the wrong IP address.

Affects dfl-2.00 and up.

#3407 The IDS engine could give false positives for some types of signatures.

Affects dfl-2.00 and up.

#3492 HighAvailability (HA) didn't always work as expected.

Affects DFL-1600/2500 and dfl-2.03 and dfl-2.04.

#3504 ZoneDefense: The firewall failed to reset the lowest used MAC and IP profile after a "save and activate".

Affects dfl-2.00 and up.

#3538 The DHCP client did not accept leases that not included a gateway.

Affects dfl-2.00 and up.

#3569 Editing ARP table entries without changing the MAC address gave an error when the configuration was saved.

Affects dfl-2.00 and up.

#3589 When downloading a configuration backup from the firewall, some extra garbage was appended to the end of the file. Restoring the configuration using the backup file worked as it should, but the size of the file was larger that required.

Affects dfl-2.00 and up.

#3636 ZoneDefense: The minimum required firmware version for DGS-3324SR/SRi, DXS-3326GSR and DXS-3350SR is changed from 4.10B15 to 4.20B14.

Affects DFL-800/1600/2500.

#3647 A reset or firmware upgrade did not log the username or IP address of the user that requested the action.

Affects dfl-2.00 and up.

#3651 When setting Daylight Saving Time (DST) the firewall required that the start

month was before the end month. That is however only valid for the northern hemisphere. In the southern hemisphere the start month is after the end month. In Australia (southern) the DST period starts in October and ends in March while the opposite is true for Europe (northern).

Affects dfl-2.00 and up.

Minor bug fixes

#3313 The wizard did not trigger a refresh of the main window after it finished. Information in the main page like configuration version and last restart was not updated.

Affects dfl-2.00 and up.

#3320 The Update Now button on the IDS Updates page did not work in all browsers.

Affects dfl-2.00 and up.

#3326 The close button in the setup wizard did not work in all browsers.

Affects dfl-2.00 and up.

#3381 L2TP server/client could use Session ID = 0, which is not allowed according to RFC 2661.

Affects dfl-2.00 and up.

#3388 In some upgraded firewalls, the link to D-Links security portal became wrong. The window opened when the "register" button on the IDS update page was clicked, would show a "404:Page not found error".

Affects dfl-2.04 and up.

Changes

#3122 A warning has been added when multiple L2TP/PPTP servers listening on the same IP has been configured.

#3331 It was only possible to enable IDS autoupdate if at least one IDS rule was added. IDS autoupdate can now always be enabled.

#3364 The front panel texts for linkspeed and uptime have been changed.

#3379 A popup alert has been added to inform the user that he needs to register his firewall on D-Links security portal.

#3380 It is now possible to set the MAC address and MTU manually for Ethernet interfaces. Note that the MAC address should not be changed unless it is required by the ISP.

#3418 Support for fast reauth in EAP negotiation has been added.

#3431 ZoneDefense: Support for DGS-3400 has been added.

Affects DFL-800/1600/2500.

#3432 ZoneDefense: Support for DXS-3300 series added. Minimum firmware requirement for DES-3350SR changed to R3.02B12, DES-3526 changed to R3.06B20, DES-3550 changed to R3.05B36, DES-3800 Series changed to R1.00B31.

Affects DFL-800/1600/2500.

#3442 The validation check made by the HTTP ALG that all characters are correctly UTF-8 encoded is now optional.

#3577 From firmware version 2.05 it will no longer be possible to upload IDS database files manually in the webUI. The updates will be downloaded automatically by the firewall, when automatic updates have been enabled.

#3674 The default value for ALG max sessions is changed to 200.

Firmware: 2.04.00

Hardware: A1
Date: Nov 22, 2005

Changes from DFL-800/1600/2500 v2.03.00 to v2.04.00

Bug fixes

#2739 WebUI: The delete option in the right-click menu has been disabled for entries in the web user interface that can't be deleted.

#2847 SMTPLog: The email recipients of the SMTP Log receiver were not configured correctly in the web user interface, which caused invalid email headers to SMTP Log receivers.

Affects dfl-2.00 and up.

#2935 SLB: Server Load Balancing did not log all changes that occurred to the health status of monitored servers.

Affects dfl-2.00 and up.

#2979 HTTP ALG: The HTTP ALG now allows compressed data. The HTTP ALG always asked the web server not to send compressed data as this does not work with content stripping. As of 2.04, the HTTP ALG will allow the server to send compressed data as long as the HTTP ALG isn't configured to do content stripping. This means that compressed data is allowed as long as the HTTP ALG isn't configured to perform stripping of ActiveX objects, Java Applets and Javascripts/VBScripts.

Affects dfl-2.00 and up.

#2989 Firewall: The Nessus test utility triggered a timing bug in the TCP stack which could cause the firewall to malfunction.

Affects dfl-2.00 and up.

#3043 Transparent mode: Redirecting traffic between two interfaces that are part of a Security/Transport equivalent interface group did not work when the

interfaces are running in Transparent Mode.

Affects dfl-2.00 and up.

#3048 Threshold: Under some circumstances, when thresholds limiting the number of new connections per second was exceeded, many log events could be sent. The new improved implementation limits the number of duplicate log events.

Affects dfl-2.00 and up.

#3156 Transparent mode: Transparent Mode feature can cause memory leakage. If excessive amounts of memory are consumed to the point that the system is out of memory, the firewall will eventually cease to work correctly and finally reboot.

Affects dfl-2.00 and up.

#3200 ARP: ARP handling in Transparent Mode incompatible with Microsoft Network Load Balancing. Microsoft NLB sends ARP queries with a source MAC address in the ARP data that differs from the source address in the Ethernet header. The firewall only allows ARP responses sent to the MAC address found in the Ethernet header of the ARP query. When hosts on the other side of the firewall sends ARP responses to the MAC address found in the ARP data the responses are dropped instead of forwarded back to the original querier.

Affects dfl-2.00 and up.

#3233 Threshold: Threshold rules could cause the firewall to malfunction when many new connections from different source IPs were spawned in a short period of time.

Affects dfl-2.00 and up.

#3244 Date and Time: Time sync servers were only parsed correct if a net object from the address book was used, not if the IP or DNS name was specified directly in the textbox.

Affects dfl-2.00 and up.

#3254 DynDNS.org client: Only hostnames using the DynDNS.org domain was supported (eg test.dyndns.org). DynDNS.org also has a lot of other domain names to choose from, and all of them are now possible to use.

Affects dfl-2.00 and up

Minor bug fixes

#3065 WebUI: Network object groups were not available in dropdown menus on some interface pages (Remote Network: Ethernet, VLAN, PPPoE client, L2TP/PPTP client and Allowed Networks: L2TP/PPTP server).

Affects dfl-2.00 and up

#3155 SMTPLog: It was possible to configure mail subjects with up to 256 characters in the webUI, but only the first 32 characters was used by the firewall. The firewall also sent empty X-Mailer and Identity values to the mail server.

Affects dfl-2.00 and up

Changes

#2871 WebUI: The URLs to the online manual and help has been changed.

Affects dfl-2.00 and up

#2897 Configuration: It is now possible to reset only the firewall configuration to factory default. Previously both firmware and configuration had to be reset. The new option is available in both the boot menu (serial console) and the webUI.

#2943 WebUI: The time the firewall will wait until it reverts the last configuration change after a "save and activate" is now user configurable. The default value for the revert timeout is 30 seconds.

#2984 IPsec: The default values for IKE and IPsec life times have been changed to 28000 seconds and 3600 seconds.

#3033 IDS: The default action for a IDS rule is changed to audit.

#3047 IDS: The possibility to trigger ZoneDefense via the Intrusion Detection System was added. The intruder's source IP address is blocked via ZoneDefense.

#3053 IDS: IDS events can now be logged to a special memory log receiver which can be browsed at the IDS Status page in the web user interface. Only IDS-related events (including thresholds) are logged to this particular memory log receiver.

#3067 ZoneDefense: Support for DES-3828 has been added. Note that switches using firmware version 1.00B23 and earlier will need a firmware upgrade in the switch to be able to use full ZoneDefense support.

#3071 IDS Update: The last 10 auto update attempts are now logged in a separate history log on the Status->IDS page. In previous firmware versions only the last attempt was shown on the status pages.

#3078 SNMP: "SNMP Before Rules" is now enabled in the default configuration.

#3089 Front panel: The time format (for current time) shown on the front panel has been changed to "Time: hh:mm".

Affects: DFL-1600 and DFL-2500

#3130 SMTPLog: A simple verification of the entered email address has been added. This verification will check that the user input at least follows the basic structure that an email address needs to have.

#3134 IDS: An unique ID has been added to all signatures. This ID will be displayed in the log when a signature triggers. To find the corresponding

advisory, a search can be performed in D-Links security portal using the logged ID or signature name.

#3145 IDS update: To continue to receive automatic IDS signature databases updates, the firewall needs to be registered in D-Links security portal. A button has been added on the IDS Updates page that will direct the user to the correct webpage.

#3146 IDS: A new button has been added on the IDS update settings page. The button can be used to manually trigger an IDS signature database update request.

#3191 ZoneDefense: Support for DHS-3618 and DHS-3626 has been added.

#3215 IDS: The IDS auto update server is no longer user configurable.

#3225 DHCP Server: It is now possible to configure default gateway and/or DNS server when running the setup wizard.